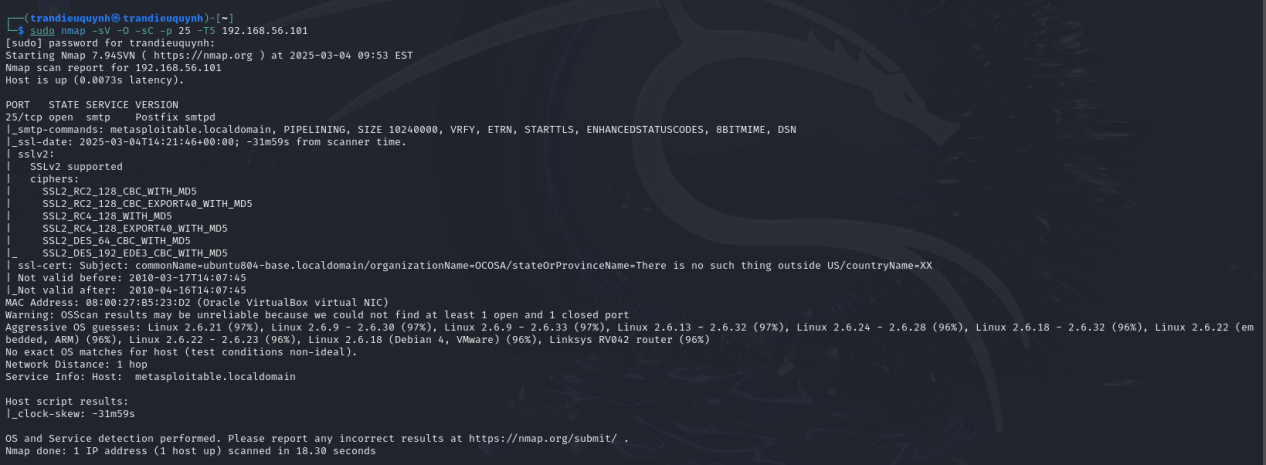
SMTP PORT 25

Service Scan with nmap

sudo nmap -sV -O -sC -p 25 -T5 <target>



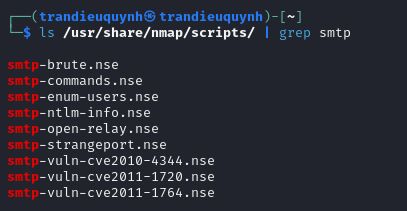
Nhận xét :

· **Port 25 (SMTP) mở** trên **192.168.56.101** → Máy chủ này đang chạy một dịch vụ SMTP.

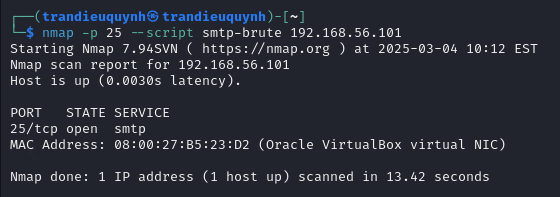
· **Dịch vụ SMTP chạy trên Postfix** (Mail Transfer Agent phổ biến).

· Hỗ trợ nhiều tính năng bảo mật như **STARTTLS, VRFY, PIPELINING, DSN**.

Hiển thị danh sách tất cả các **Nmap script** liên quan đến SMTP



--script smtp-brute



Nhận xét

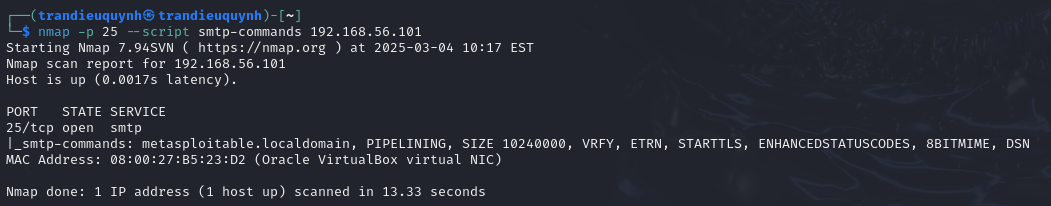
Không có kết quả nào từ smtp-brute, nghĩa là:

Máy chủ SMTP không yêu cầu xác thực hoặc

Không có danh sách username/password để thử brute-force

Dịch vụ SMTP đã chặn brute-force (có thể do bảo mật)

smtp-commands



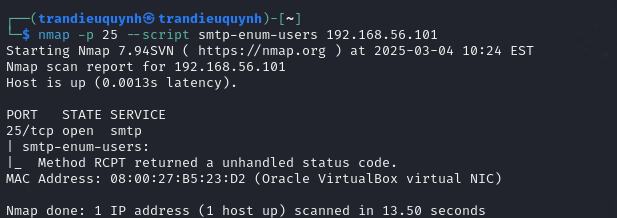
Nhận xét

· Máy chủ **192.168.56.101** đang **mở cổng 25 (SMTP)**.

· Danh sách lệnh SMTP được hỗ trợ:

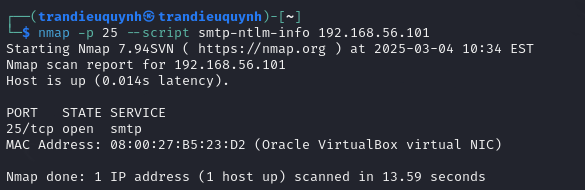
* **PIPELINING**: Cho phép gửi nhiều lệnh SMTP mà không cần chờ phản hồi từng lệnh.
* **SIZE 10240000**: Hỗ trợ gửi email với dung lượng tối đa **10MB**.
* **VRFY**: Có thể kiểm tra xem một địa chỉ email có tồn tại hay không.
* **ETRN**: Hỗ trợ mail queue flushing (đẩy email bị tạm dừng).
* **STARTTLS**: Hỗ trợ mã hóa TLS để bảo mật kết nối.
* **ENHANCEDSTATUSCODES**: Hỗ trợ mã trạng thái SMTP mở rộng.
* **8BITMIME**: Hỗ trợ gửi email với nội dung 8-bit thay vì 7-bit.
* **DSN**: Hỗ trợ thông báo trạng thái gửi email.

smtp-enum-users



Nhận xét

smtp-ntlm-info



Enumerating users (manually)